UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/654,417	09/04/2003	Philip Kwan	FOUND-0058 (034103-049)	7628

49680 7590 12/31/2007

FOUNDRY-THELEN REID BROWN RAYSMAN & STEINER LLP
P.O. BOX 640640
SAN JOSE, CA 95164-0640

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
12/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/654,417	KWAN ET AL.	
	Examiner	Art Unit	
	Shanto M Z Abedin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/22/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application on 10/22/2007, after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

2. The examiner notes, a terminal disclosure was filed by the applicant on 03/20/2007 to overcome the obvious type double patenting with the co-pending application No. 10/458,628, and subsequently the previous obvious type double patenting rejection was withdrawn.

3. Claims 1- 46 are currently pending in the application.

4. Claims 1-46 are rejected.

Response to Arguments

4. The applicant's arguments regarding the previous 35 U.S.C. 102(e) and 103(a) type rejections of claims 1-43 are fully considered, however, they are moot in view of new grounds of rejection presented in this office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-3, 6-7,11 ,13-15, 17, 23-25, 28-29 and 44-46 are rejected under 35 USC 103 (a) as being unpatentable over Kanuri et al (US 6807,179 B1) in view of Short et al (US 7194554 B1).

Regarding claim 1, Kanuri et al teaches a layer 2 network access device for providing network security, comprising:

a plurality of input ports (Fig1, 12.22; Col 3, lines 25-67; multiport switch)

a switching fabric in the layer 2 network access device for routing data received on said plurality of input ports to at least one output port (Fig 1.28; Col 3, lines 25-67; switch fabric; Col 4, lines 7-52; layer 2 switch); and

control logic in the layer 2 network access device (Col 3, line 28 to Col 5, line 65: the switch; MAC module; switching (rules) logic) adapted to authenticate a physical address of a user device coupled to one of said plurality of input ports (Col 3, line 28 to Col 5, line 65; matching MAC addresses), to authenticate user information provided by a user of said user device only if said physical address is valid (Col 3, line 54 to Col 4, line 34; Col 5, lines 10-65; user, or network nodes' attributes/ policies/ information; user defined policies/ attributes; authenticating VLAN field/ index/ information, and MAC addresses specific to user/ network node/ data frame), and to restrict access to said one of said plurality of input ports in accordance with a user policy associated with said user information only if said user information is valid (Fig 2:40; associated port, MAC and VLAN information; Fig 3, step 70-106; Col 5, lines 43-60; if in step 74 the switching rules logic determined a match between MAC...VLAN index....(then) checks in step 76 whether port ...; the examiner interprets switching "rules" logic as policy; port filtering).

In the case, obviousness regarding authenticating user provided authentication information, and MAC is not found to be supportive, the examiner notes, Short et al discloses network security/ access device authenticating user provided authentication information, and MAC (Fig 2; Col 4, starts at line 12; authentication; user id; MAC).

Short et al and Kanuri et al are analogous art because they are from the same field of endeavor of secure network communication. At the time of invention, it will be obvious to a person of ordinary skill in the art to combine the teachings of Short et al with Kanuri to design an apparatus wherein network security/ access device authenticates user provided authentication information, and MAC in order to provide further security to the system.

Regarding claim 13, it is rejected applying as above as rejecting claim 1, furthermore, Kanuri et al teaches a method for providing network security, comprising:

authenticating in a laver 2 network access device a physical address of a user device coupled to a port of a the network access device (Fig 2:40; associated port, MAC and VLAN information; Col 3, line 28 to Col 5, line 65; matching MAC addresses);

authenticating user information provided by a user of said user device to the network access device only if said physical address is valid (Col 3, line 54 to Col 4, line 34; Col 5, lines 10-65; user or network nodes' attributes/ policies/ information; user defined policies/ attributes; authenticating VLAN field/ index/ information, and MAC addresses specific to user/ network node/ data frame); and

restricting access to said port in accordance with a user policy associated with said user information only if said user information is valid (Fig 2:40; associated port, MAC and VLAN information; Fig 3, step 70-106; Col 5, lines 43-60; if in step 74 the switching rules logic determined a match between MAC...VLAN index....(then) checks in step 76 whether port ...; the examiner interprets switching "rules" logic as policy; port filtering).

In the case, obviousness regarding authenticating user provided authentication information, and MAC is not found to be supportive, the examiner notes, Short et al discloses network security/ access device authenticating user provided authentication information, and MAC (Fig 2; Col 4, starts at line 12; authentication; user id; MAC).

Regarding claim 23, it is rejected applying as above rejecting claim 1, furthermore, Kanuri et al teaches network system, comprising:

a data communications network (Fig 1; Col 3, line 27 to Col 4, line 50; communication between network nodes/ stations/ devices);

a layer2 network access device coupled to said data communications network (Fig 1.28; Col 3, lines 25-67; switch fabric; Col 4, lines 7-52; layer 2 switch); and

a user device coupled to a port of said network access device (Col 3, line 54 to Col 4, line 34; user, or network nodes' attributes/ policies/ information);

wherein said network access device is adapted to authenticate a physical address of said user device (Col 3, line 28 to Col 5, line 65; matching MAC addresses), to authenticate user information

provided by a user of said user device only if said physical address is valid (Col 3, line 54 to Col 4, line 34; Col 5, lines 10-65; user, or network nodes; user defined policies/ attributes; authenticating VLAN field/ index/ information, and MAC addresses specific to user/ network node/ data frame), and to restrict access to said port in accordance with a user policy associated with said user information only if said user information is valid (Fig 3, step 70-106; Col 5, lines 43-60; if in step 74 the switching rules logic determined a match between MAC...VLAN index....(then) checks in step 76 whether port ...; the examiner interprets switching "rules" logic as policy).

In the case, obviousness regarding authenticating user provided authentication information, and MAC is not found to be supportive, the examiner notes, Short et al discloses network security/ access device authenticating user provided authentication information, and MAC (Fig 2; Col 4, starts at line 12; authentication; user id; MAC).

Regarding claim 2, Kanuri et al teaches the network access device of claim 1, wherein said physical address comprises a Media Access Control (MAC) address (Col 5, starts at line 23; MAC address).

Regarding claim 3, Kanuri et al teaches the network access device of claim 1, wherein said control logic is adapted to authenticate said user information in accordance with an IEEE 802. lx protocol (Col 3, starting at line 36: IEEE 802.3).

Regarding claim 6, Kanuri et al teaches the network access device of claim 1, wherein said user policy identifies a Media Access Control (MAC) address filter (Fig 2.40, 2.42; Col 5, starting at line 41; address table including MAC/ VLAN/ Port information; matching MAC addresses) .

Regarding claim 7, Kanuri et al teaches the network access device of claim 1, wherein said user policy includes a Media Access Control (MAC) address filter (Fig 2.40, 2.42; Col 5, starting at line 41; address table including MAC/ VLAN/ Port information; matching MAC addresses).

Regarding claim 11, Kanuri et al teaches the network access device of claim 1, wherein said control logic is further adapted to assign said one of said plurality of input ports to a virtual local area network (ULAN) associated with said user information if said user information is valid (Col 5, starting at line 25; matching VLAN information).

Regarding claims 14-15, 17, 24-25, 28-29, they recite the limitations of claims 1-3, 6-7, therefore, they are rejected applying as above rejecting claims 1-3 and 6-7.

Regarding claims 44, 45 and 46, they are rejected applying as above rejecting claims 1,13 and 23, furthermore, Short et al discloses user information comprises user name and password (Col 8, starts at line 10)

6. Claims 4-5, 16, 26 and 27 are rejected under 35 USC 103 (a) as being unpatentable over Kanuri et al (US 6807,179 B1) in view of Short et al (US 7194554 B1) further in view of Mate et al (US 7028098 B2) further in view of Gai et al (US 2004/0160903 A1)

Regarding claim 4, Kanuri et al fails to disclose network access device wherein said user policy identifies an access control list.

However, Mate et al discloses network access device wherein said user policy identifies an access control list (Col 5, starts at line 60; Col 10, starts at line 45; policy; ACL).

Furthermore, Gai et al discloses network access device wherein said user policy identifies an access control list (Fig 5; Fig 6B; Par 0007-0008; 0039, 0046; ACL)

Gai et al , Mate et al and Kanuri et al are analogous art because they are from the same field of endeavor of secure network communication. At the time of invention, it will be obvious to a person of ordinary skill in the art to combine the teachings of Mate et al or Gai et al with modified Short et al – Kanuri system to design an apparatus wherein user policy identifies an access control list to facilitate a managed packet filtering based on port or flow information.

Regarding claim 5, Kanuri et al fails to disclose the network access device wherein said user policy includes an access control list (Col 5, starts at line 60; Col 10, starts at line 45; policy ..including ACL).

Regarding claims 16, 26 and 27, they recite the limitations of claims 4 and 5, therefore, they are rejected applying as above rejecting claims 4 and 5.

7. Claims 8-10, 12, 18-22, 30-34 are rejected under 35 USC 103 (a) as being unpatentable over Kanuri et al (US 6807,179 B1) in view of Short et al (US 7194554 B1) further in view of See et al (US6874090 B2).

Regarding claim 8, Kanuri et al fails to teach the network access device of claim 1, wherein said control logic is adapted to send said user information to an authentication server and to receive an accept message from said authentication server if said user information is valid.

However, See et al teaches control logic is adapted to send said user information to an authentication server and to receive an accept message from said authentication server if said user

information is valid (Col 6, starting at line 32; Col 10, starting at line 10; claims 25-27; authentication information including VLAN identifier; user identification information).

Furthermore, Short et al teaches control logic is adapted to send said user information to an authentication server and to receive an accept message from said authentication server if said user information is valid (Col 3, starts at line 10; AAA / RADIUS server authenticating user id).

Short et al , See et al and Kanuri et al are analogous art because they are from the same field of endeavor of secure network communication. At the time of invention, it will be obvious to a person of ordinary skill in the art to combine the teachings of See et al with modified Short et al - Kanuri system to design an apparatus further including an authentication server in order to facilitate proper VLAN authentication.

Regarding claim 9, Kanuri et al fails to teach the network access device of claim 8, wherein said authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server.

However, See et al teaches wherein said authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server (Col 10, starting at line 10; claims 25-27).

Regarding claim 10, See et al teaches wherein said accept message includes said user policy (Col 1, starting at line 56).

Regarding claim 12, See et al teaches the network access device of claim 11, wherein said control logic is adapted to receive a message from an authentication server, wherein said message comprises a VLAN identifier (ID) associated with said user information, and to assign said one of said plurality of input ports to a ULAN associated with said VLAN ID (Col 6, starting at line 32; Col

10, starting at line 10; claims 25-27; VLAN identifier; user identification information; authentication server, information). Furthermore, Short et al discloses wherein said message comprises a VLAN identifier (ID) associated with said user information, and to assign said one of said plurality of input ports to a ULAN associated with said VLAN ID (Col 3, starts at line 10; VLAN ID)

Regarding claims 18-22, 30-34, they recite the limitations of claims 8-10 and 12, therefore, they are rejected applying as above rejecting claims 8-10 and 12.

8. Claims 35-37 are rejected under 35 USC 103 (a) as being unpatentable over Kanuri et al (US 6807,179 B1) in view of Short et al (US 7194554 B1) further in view of See et al (US6874090 B2) further in view of Volpano (US 7188364 B2).

Regarding claims 35-37, they are rejected applying as above rejecting claims 1, 14 and 24. Furthermore, Kanuri et al discloses network access device/ method/ apparatus wherein said control logic is further configured to:

if authentication of said MAC address indicates said MAC address is invalid (Fig 3, step 70-106; Col 5, lines 43-60; authenticating MAC address); or

disable said port (Col 5, starts at line 40; disabling port).

Kanuri et al fails to disclose

if authentication of said user information indicates said user information is invalid, block all traffic on said port except for packets related to a user authentication protocol; if authentication of user information indicates said user information is valid, determine whether said user is associated with a VLAN supported by said network access device;

if said user is not associated with said VLAN, assign said port to a port default VLAN; and block all traffic on said port except for packets related to said user authentication protocol; and

if said user is associated with said VLAN, assign said port to said VLAN associated with said user; and forward packets from said user device.

However, Short et al discloses if authentication of user information indicates said user information is valid, determine whether said user is associated with a VLAN supported by said network access device (Col 3, starts at line 12; packet transmission; VLAN, user Id authenticating); and if said user is associated with said VLAN, assign said port to said VLAN associated with said user; and forward packets from said user device (Col 3, starts at line 12).

Furthermore, See et al discloses dropping packets if MAC address is not valid, if authentication of user information indicates said user information is valid, determine whether said user is associated with a VLAN supported by said network access device ; and if said user is associated with said VLAN, assign said port to said VLAN associated with said user; and forward packets from said user device (Col 3, starts at line 10; authenticating user identification information in VLAN; packet transmission).

Modified Short et al-Kanuri system fails to disclose

if authentication of said user information indicates said user information is invalid, block all traffic on said port except for packets related to a user authentication protocol; and if said user is not associated with said VLAN, assign said port to a port default VLAN; and block all traffic on said port except for packets related to said user authentication protocol;

However, Volpano discloses if authentication of said user information indicates said user information is invalid, block all traffic on said port except for packets related to a user authentication protocol; and if said user is not associated with said VLAN, assign said port to a port default VLAN; and block all traffic on said port except for packets related to said user authentication protocol (Col 5, starting at line 30; control frames; EAPOL).

Volpano and Kanuri et al are analogous art because they are from the same field of endeavor of VLAN utilizing bridges/ switches. At the time of invention, it will be obvious to a person of ordinary skill in the art to combine the teachings of Volpano with modified See at al – Short et al - Kanuri et al apparatus/ method/ system to design an apparatus further adapted to drop/ filter packets by authenticating utilizing an authentication server, authentication protocol message containing VLAN identifier in order to provide a proper VLAN packet filtering.

9. Claims 38-43 are rejected under 35 USC 103 (a) as being unpatentable over Kanuri et al (US 6807,179 B1) in view of Short et al (US 7194554 B1) in view of See et al (US 6874090 B2) further in view of Volpano (US 7188364 B2).

Regarding claims 38, 40 and 42, Kanuri et al teaches an apparatus/ method/ system for providing network security, comprising:

A data communication network (Col 3, starts at line 26; network packets);

A network access device coupled to said data communication network (Col 3, starts at line 26; switch enabling communication);

a plurality of input ports (Fig1, 12.22; Col 3, lines 25-67; multiport switch);

a switching fabric for routing data received on said plurality of input ports to at least one output port (Fig 1.28; Col 3, lines 25-67; switch fabric; Col 4, lines 7-52; layer 2 switch); and

control logic adapted to:

authenticate a physical address of a user device coupled to one of said plurality of input ports (Col 3, line 28 to Col 5, line 65: the switch; MAC module; switching (rules) logic; matching MAC addresses);

authenticate user information provided by a user of said user device only if said physical address is valid (Col 3, line 54 to Col 4, line 34; Col 5, lines 10-65; user or network nodes' attributes/ policies/ information; user defined policies/ attributes; authenticating VLAN field/ index/ information, and MAC addresses specific to user/ network node/ data frame);

if authentication of user information indicates said user information is valid, determine whether said user is associated with a VLAN supported by said apparatus, wherein said message comprises a VLAN identifier (ID) associated with said user information (Col 5, lines 1-65; determining/ matching VLAN index/ information);

if said user is associated with said VLAN,

assign said one of said plurality of ports to said VLAN associated with said user (Col 5, lines 1-20; Col 6, lines 1-40; switching logic assigning/ selecting ports);

if said user is not associated with said VLAN,

assign said one of said plurality of input ports to a port default VLAN (Col 5, lines 1-20; Col 6, lines 1-40; switching logic assigning/ selecting ports); and

restrict access to said one of said plurality of input ports in accordance with a user policy associated with said user information (Fig 2:40; associated port, MAC and VLAN information; Fig 3, step 70-106; Col 5, lines 43-60; **if** in step 74 the switching rules logic determined a match between MAC...VLAN index....(then) checks in step 76 whether port ...; the examiner interprets switching "rules" logic as policy; port filtering).

In the case, obviousness regarding authenticating user provided authentication information, and MAC is not found to be supportive, the examiner notes, Short et al discloses network security/ access device authenticating user provided authentication information, and MAC (Fig 2; Col 4, starts at line 12; authentication; user id; MAC).

Kanuri et al fails to disclose expressly

drop packets from said user device if said physical address is invalid;

if authentication of said user information indicates said user information is invalid, block alltraffic on said one of said plurality of input ports except for packets related to a user authentication protocol; receiving a message from an authentication server, wherein said message comprises a VLAN identifier (ID) associated with said user information;

if said user is not associated with said VLAN, block all traffic on said one of said plurality of input ports except for packets related to said user authentication protocol.

However, See et al discloses

drop packets from said user device if said physical address is invalid (Col 6, starting at line 32; filtering/ dropping packets based on MAC/ VLAN identifier) ;

receiving a message from an authentication server, wherein said message comprises a VLAN identifier (ID) associated with said user information (Col 6, starting at line 32; Col 10, starting at line 10; claims 25-27; authentication information including VLAN identifier; user identification information);

Modified See at al – Short et al- Kanuri et al apparatus/ method/ system fails to disclose

if authentication of said user information indicates said user information is invalid, block all traffic on said one of said plurality of input ports except for packets related to a user authentication protocol.

if said user is not associated with said VLAN, block all traffic on said one of said plurality of input ports except for packets related to said user authentication protocol.

However; Volpano discloses

if authentication of said user information indicates said user information is invalid, block all traffic on said one of said plurality of input ports except for packets related to a user

authentication protocol (Col 5, starting at line 30; control frames; EAPOL);

if said user is not associated with said VLAN,

block all traffic on said one of said plurality of input ports except for packets related to said

user authentication protocol (Col 5, starting at line 30; control frames; EAPOL).

Volpano and Kanuri et al are analogous art because they are from the same field of endeavor of VLAN utilizing bridges/ switches. At the time of invention, it will be obvious to a person of ordinary skill in the art to combine the teachings of modified See at al – Short et al-Kanuri et al apparatus/ method/ system with Volpano to design an apparatus further adapted to drop/ filter

packets by authenticating utilizing an authentication server, authentication protocol message containing VLAN identifier in order to provide a proper VLAN packet filtering.

Regarding claims 39, 41 and 43, Kanuri et al discloses wherein said network access device comprises a layer 2 network access device (Col 3, starts at line 27; the multiport switch enabling communication of layer 2 type data packets; layer 2 switch).

Conclusion

10. A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDOMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system,

see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, AU 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

12/25/07